The agency owners' guide to site security

How to prevent security issues when managing multiple sites.

Nimbus

Contents

Who is Nimbus?

We provide eco-friendly managed web hosting specifically for ambitious UK agencies and freelancers.

Everything we do is designed to make things simple, and keep your sites super fast, reliable and secure.

Host any PHP-based site with **100% root access** to your server and enjoy **99.995% uptime**, all without damaging the planet, since our data centres run on 100% renewable energy.

We back it all up with a platform packed with useful tools - not to mention - plus our **UK-based support**: real people, full of hosting know-how, and ready to answer questions in less than an hour.

We're also **carbon neutral**, meaning hosting with us isn't just a good choice for your team, it's a good choice for the planet, too.

So if you're the superhero for your clients, think of us as your behind-the-scenes support team.

Simple, green, and reliable.

Authors

NICK FORD,
Head of DevOps & Infrastructure

Nick is Head of DevOps & Infrastructure at Nimbus. He is responsible for ensuring all our systems are achieving maximum uptime and performance, and acts as a technical escalation point for all teams.

Over the last 9 years he has been working to automate processes within the company, from server builds to zero downtime platform deployments. Nick is always test-driving new technologies and finding systems which can take Nimbus services to the next level.

LUKE TONKIN,
DevOps & Infrastructure Engineer

Luke has been working in hosting for 8 years and currently sits within our DevOps & Infrastructure team. He is responsible for the hardware and networking infrastructure at Nimbus, working behind the scenes to keep everything running smoothly.

Luke is passionate about servers and new technologies, and loves to tinker with anything to do with computers in his spare time.

An introduction to site security.

Securing your websites against online threats is a somewhat complex process that requires you to constantly outpace new dangers as they develop.

Fall behind and your shields become less effective, making your CMS vulnerable and putting your sites at risk of attacks.

Establishing good site security therefore means introducing **several layers of protection** to cover specific scenarios and infrastructure elements.

Like server access and PCI Compliance, you need a digital environment with maximum protection from various attacks, hacks, and instances of fraud

This is especially true of sites built in **WordPress**. The CMS's popularity means that it's a prime target for malicious attacks. WordPress security flaws are rife if you don't take care to add the right plugins and protections.

WordPress is the most popular CMS in the world. Over 455 million sites[1] use it (as of 2021), and it powers 37% of all websites globally.

[1] https://www.envisagedigital.co.uk/wordpress-market-share/

This is the case with other open-source software too, such as Magento. Because these softwares release their source code to the general public, hackers can study them for vulnerabilities, which can make them easier to breach.

The good news? With proper security precautions, you can protect your sites from attacks regardless of the software they're built in.

As hosting geeks, we're always thinking about how to better ensure site security. **In fact, we've built multiple tools right into our hosting platform to help our customers protect their builds. Our support team is always on hand to support our agency and freelancer customers to improve security for their clients.**

We know that being able to rely on expert knowledge can alleviate some of the pressure involved in managing multiple sites.

So with that in mind, we've pulled together a list of recommendations, expert tips, and even a guide to the best WordPress security plugins, all to help you ensure that your multi-site portfolio is protected.

NICK FORD,
Head of DevOps & Infrastructure

Web Application Firewalls.

Web Application Firewalls (WAFs) provide base-level protection to **web applications** by filtering the HTTP traffic that comes from the internet, preventing many common attacks.

Web Application Firewalls (WAFs) are a type of reverse proxy – think of them as a barrier between the server and your client's website. They run on a set of policies which dictate what kind of traffic they should filter out, protecting the servers by blocking malicious traffic from hitting them.

As WAFs are a highly responsive form of protection that can be easily modified, they are particularly useful on high-traffic sites.

While a WAF is not enough to guarantee site security on its own, it forms an important part of a larger security protocol, and can often help to mitigate the risks of attacks such as cross-site forgery, cross-site-scripting, file inclusion, and SQL injection.

Speak to your dev team about ensuring WAFs are active across your portfolio of client websites.

At Nimbus, we often recommend customers use Cloudflare's WAF on their clients' sites.

As a cloud-based solution, it's continuously updated to protect against the newest threats, which means that there's one less thing for you to worry about.

Did you know?
It's thought that as many as 30,000 websites are hacked every day[2].

[2] https://spanning.com/blog/cyberattacks-2021-phishing-ransomware-data-breach-statistics/

Continual updates.

The most common vulnerability seen across WordPress sites is running an outdated version.

In fact, this is true of any open-source software.

After Magento 1 was phased out and stopped receiving security patches, nearly 3,000 Magento 1 stores[3] were hit by attacks.

As new patches and updates are released, it's important to ensure that your open-source software and WordPress sites are up-to-date, as these updates will address known security issues and vulnerabilities within the software.

Although a relatively simple preventative measure against the threat of having your WordPress site hacked, these updates are necessary to monitor your entire ecosystem: WordPress core files, versions, themes, and each of your chosen plugins.

At Nimbus, our platform alerts users about out-of-date software from the WordPress dashboard, where you can then implement updates at the press of a button.

This makes bulk management much easier, which is crucial – updates should be implemented as soon as possible to reduce the risk of cyber attacks resulting from compromised software.

If your hosting partner doesn't include a notification service, third-party applications such as **WP Manager** can be used to manage all of your themes and plugins. This means you won't need to manually check for updates across your entire portfolio.

They usually come with an additional cost, though, so make sure to factor that into your platform budgeting.

Did you know?

53.6% of WordPress sites are not yet running the latest version[4].

[3] https://www.bigcommerce.co.uk/articles/ecommerce/ecommerce-data-breaches/#ecommerce-data-breaches-examples-and-statistics-

[4] https://wordpress.org/about/stats/

DOWNLOAD INSIGHT REPORT

Why you should offer website maintenance retainer packages.

When security is such an important factor in the continued success of your clients' sites, leaving them to manage the ongoing security updates can feel like setting you both up for a future headache.

That's why we recommend offering a retainer package as part of your client quote.

To help you, we're giving you our exclusive research into almost 200 UK agencies, demonstrating a new best practice for retainers - **The Agency Retainer Report: Actionable insight for maximising your revenue and profit with retainers.**

It contains a breakdown of agency turnovers; current averages across retainer pricing; profit margins and retainer inclusions; expert commentaries; and opportunities for growth.

It provides everything an agency needs to know to more **effectively manage their retainers and grow their profit margins.**

With a **website maintenance retainer package,** you can generate additional income while ensuring your clients' sites are kept secure - giving both them and you additional peace of mind.

When putting a retainer package together, it's important that you consider the time it will take you to keep sites updated, with allowances for **testing periods** to provide increased value to your customers.

If your websites are hosted on a platform like Nimbus, with its central view of all your sites and servers, updating everything is a relatively simple task - you can complete **bulk-updates with the push of one button.**

But some hosting platforms are more complicated and will eat up additional time, so make sure you're clear on how involved you will need to be in order to establish a reliable update schedule.

RECIPE LIST:

The best WordPress security plugins

When you're looking for the best WordPress security set-up, you'll find it very easy to fall into the plugins rabbit-hole.

There are **over 59,000 WordPress plugins[5] available**, and navigating through the list to find the best WordPress protection can take time. Time you don't have to spare, because installing your plugins straight away, rather than retrospectively, is the best way to guarantee site security.

So, to save you time and effort, we've drawn together this: **the ultimate recipe for WordPress security.**

This collection of plugins can be added to your sites to add additional security features and protections.

- **Akismet**
- **Wordfence**
- **Jetpack**
- **ReCAPTCHA**

[5] https://en-gb.wordpress.org/plugins/

Akismet

A **spam protection** plugin, Akismet, is added by default when you install WordPress. It's trusted, regularly updated, and provides a solid foundation on which to build a comprehensive plugin security recipe.

Akismet works by **cross-referencing site comments and contact form submissions against its database of spam** in order to prevent sites from publishing malicious content.

Any flagged content can then be **reviewed in your comments admin screen** - though a discard feature ensures that the most outright spam is blocked, so you save on disk space and prevent a backlog of spam from slowing your site.

Akismet is the most popular security plugin used across our clients' sites: **a third of all our WordPress sites have Akismet installed** to protect them from spam.

Wordfence

Wordfence is a WordPress **security scan** plugin that gives you total **visibility over real-time traffic, 404 errors, bots and disk space** (which can often be an indicator of a DDoS attack). It includes a two-factor authentication (2FA) for added login security, a WAF, and a scan feature which checks core files, themes and plugins for malware and other security concerns.

In the event of a security breach, Wordfence will **send alerts** to approved email addresses, meaning you or your devs can quickly respond to keep your sites secure.

It is the second most popular WordPress plugin used amongst Nimbus customers, with **22% of our WordPress clients choosing to install Wordfence** as a security measure across their portfolios.

Jetpack

Another free WordPress security plugin, Jetpack, includes a **robust backups feature** with unlimited storage, which makes it **ideal for eCommerce** stores.

Along with the usual suite of security features like an activity log, malware scans, spam protection, and DDoS attack protection, it also includes optional 2FA features for securing WordPress logins.

ReCAPTCHA

A simple yet effective **anti-bot** plugin, reCaptcha protects WordPress sites from **spam form entries** by requiring users to confirm that they are not robots before the form is able to be submitted.

It can be added to login, registration, password recovery, comment boxes, popular contact forms, and even more pages.

Focus on: site speed

Too many plugins can lengthen your sites' load time. That's not great, because slow sites lead to a higher bounce rate and worse SEO rankings, and it doesn't matter if your websites are the most secure in the world if there are no visitors to protect them for.

That's why we recommend having **no more than 20 plugins** at any one time.

Multi-server environments.

Hosting all of your clients on one server may seem cost-effective, especially when everything is running as it should be, but the reality is that this tactic can place your entire client portfolio at risk.

In fact, there are some significant benefits to splitting your clients across servers and creating a multi-server environment - a main one of which is increased security.

Here's how it works: splitting out your servers allows the resources available to be allocated more evenly amongst the hosted sites.

So if you have a large client, host complex sites, or some with a high volume of traffic, splitting these out amongst multiple servers ensures that these larger sites **don't eat up all the resources and cause downtime** for their neighbouring sites.

The security benefits work in a similar way. Should one of your sites be compromised, having the others separated out across servers means that you mitigate the risk that the one infected site will bring down the others that are sharing resource-space.

There's also the additional benefit of increased manual control over server access. Some hosting providers will give you the option to allow, time-out, or remove users and IP addresses from server access at any time - guaranteeing secure connections to a server.

On the Nimbus platform, this can be done in just a few simple clicks.

Our platform makes it easy to **view multiple servers all from one dashboard.** You can easily switch between server views, with customisable access for each - which means you can confidently reassure your clients that only the necessary people have access to their hardware, locking down their infrastructure even further.

PCI Compliance.

Ecommerce sites must comply with the Payment Card Industry Data Security Standards (PCI DSS) if they process card payments on-site without including a third-party platform (like PayPal, for example).

Ensuring that you're PCI Compliant can help you land bigger clients - so it should be a priority for any agency dealing with eCommerce sites.

Why is it so important? Well, the process of becoming PCI Compliant ensures that **payment data is encrypted and customers are protected** from instances of fraud.

That's because these regulations contribute to a globally-recognised payment data security solution, and the required steps to achieve compliance address a handful of security concerns.

In order to be PCI compliant, a site must:

- **Segment data**
- **Control access to that data**
- **Monitor the data**
- **Have an information security policy**
- **Have a secure processing network (including firewalls)**
- **Use strong access control measures (including non-default passwords and updated security settings)**

Did you know?
41% of UK customers would not return to a business following a data breach[6].

If your clients were to suffer a data breach that exposed customers' sensitive information, they could find themselves liable for damages. And it's not only the financial implications that matter in instances of data loss - the reputational damage can really affect businesses too.

On the Nimbus platform, you can prepare your infrastructure for PCI compliance testing with just the flip of a toggle, which ensures that payment data undergoes high levels of encryption while in transit.

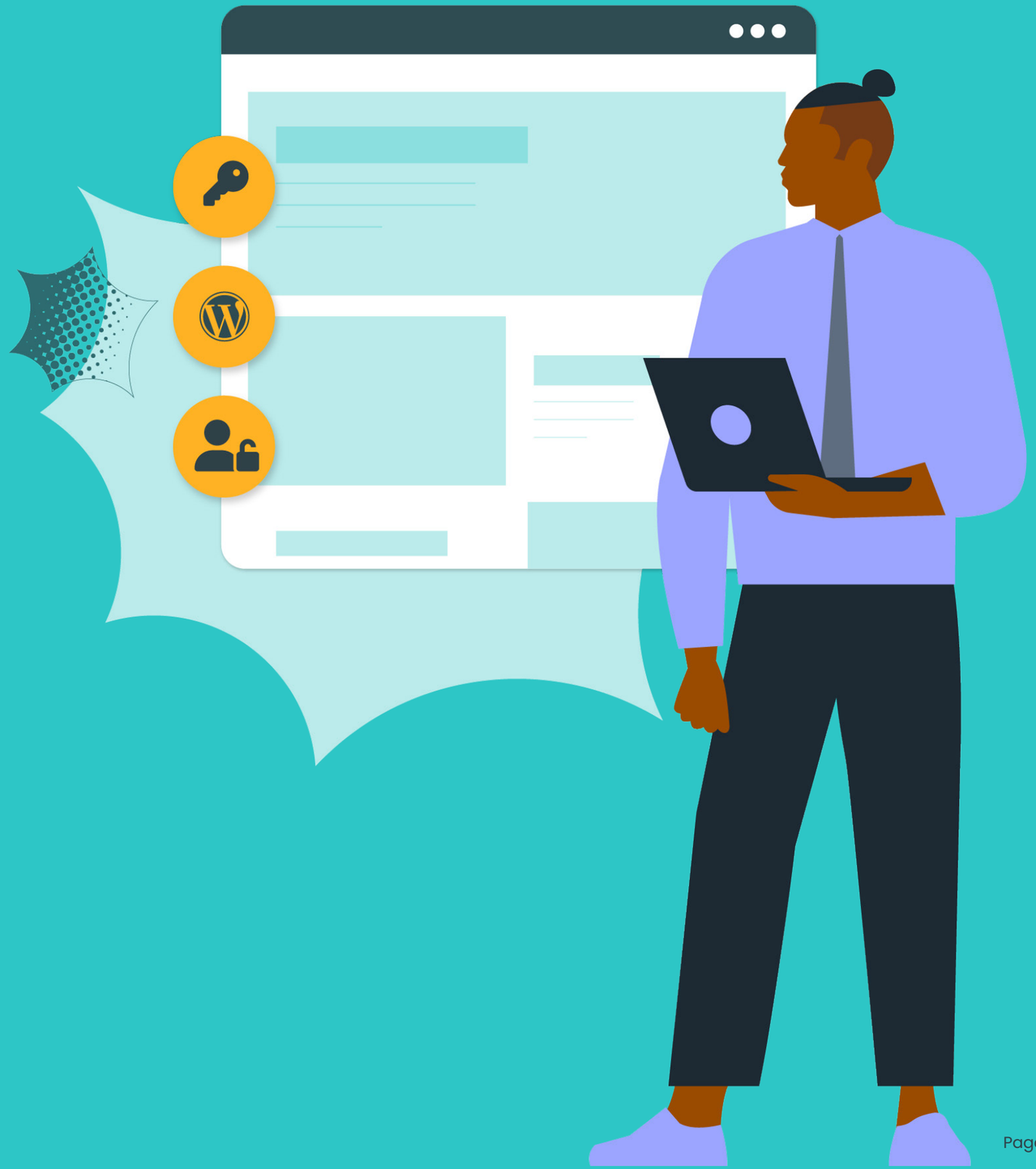
If your hosting provider doesn't offer a PCI compliance function, you'll be able to follow the steps involved in securing cardholder data at the PCI DSS website.

[6] https://www.businesswire.com/news/home/20190917005012/en/New-Global-Research-Shows-Poor-Data-Security

WordPress admin.

Hackers love when the people behind WordPress sites leave their default settings in place - it gives them a headstart on breaking in.

Things like your admin page URL, if they're not protected, remove a hurdle from any potential WordPress hacker straight away: they've found the door, now they only need to figure out the lock.



It's good practice to create a custom admin URL (and ensure your custom username is paired with a complex password).

Speak to your dev team about making some simple changes to your WordPress set-up to help promote better security. Like following your **admin URL with a string of random letters** rather than the default '/wp-admin', for example, which will give you an extra layer of protection from those attempting to access the back-end of your websites.

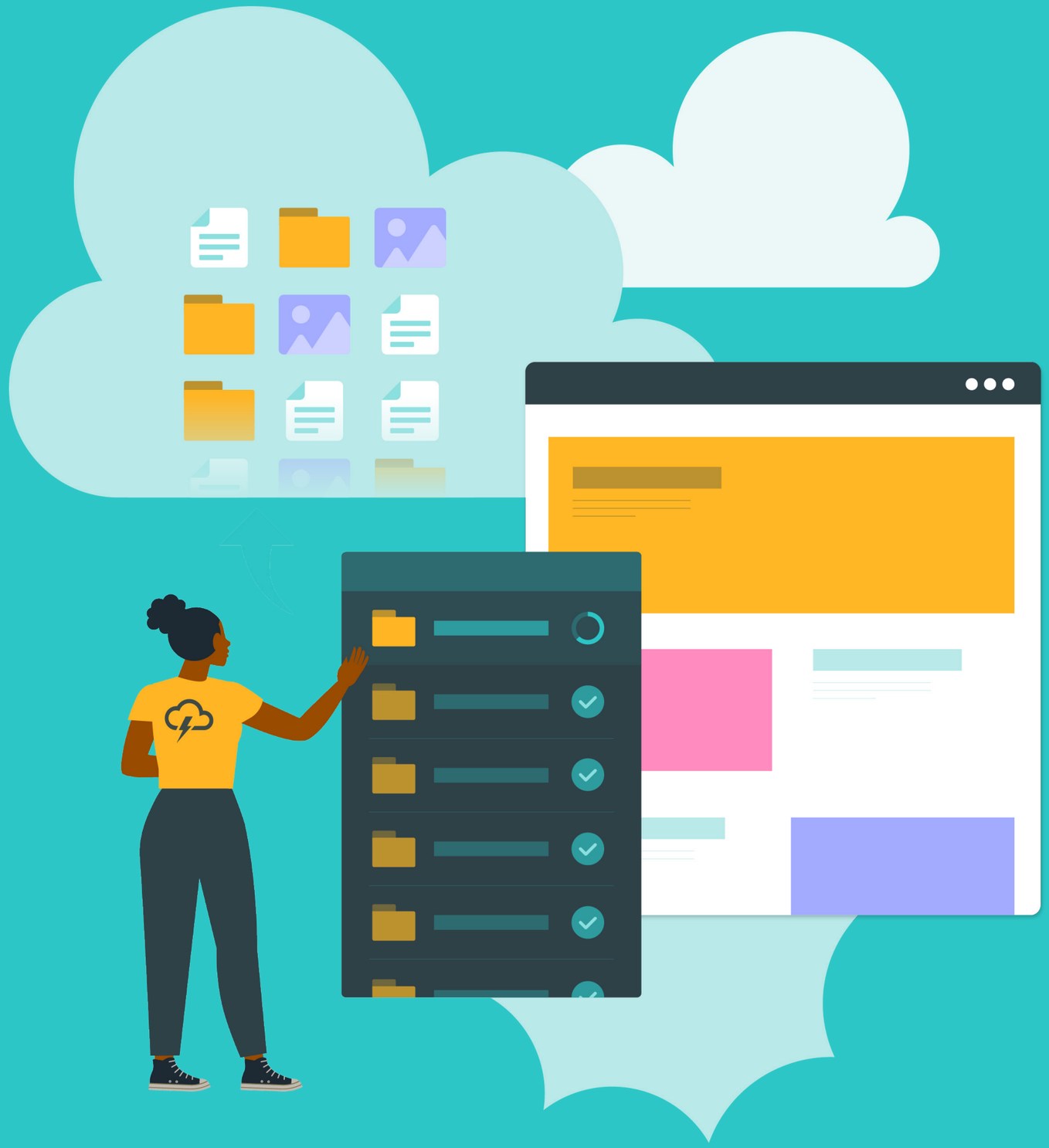
This change can be easily made using a free WordPress security plugin like **WPS Hide Login.** A change like this also has the added benefit of cutting-down on nuisance, resource-wasting bot-traffic.

To build on this extra security, we also recommend you use the **'allow from and deny from'** abilities to restrict access to the WordPress logins, and allow only specific IP addresses.

This locks down access to your admin site even further, either by removing access from suspicious IPs, or limiting access only to those IPs you trust, like those at your office.

Those not on the list will be unable to reach the page, and instead receive a **404** or 'sorry you are not allowed to access this page' message.

You'll have to make sure you have a **static IP** before defining those allowed addresses, but a feature like that is useful when opening admin access to clients without leaving the admin page without an extra security layer.



Offsite backups.

Should the worst happen, the knowledge that you have a full (and safe) site backup will save you a significant amount of stress.

It means, should anything be lost on your current site, you can restore a past version and undo the damage.

Offsite backups provide an even further layer of security, because they mean that the **copy of your site is saved at a totally different location** to your main server, meaning that even if something were to damage your website at a server-level, you wouldn't suffer complete data loss.

Not only that, but since these offsite backups don't form part of your server at a filesystem level, hackers would **never be able to access your encrypted backups.**

Offsite backups are the most effective contingency against total security failure, as their separation from your main server means that even extremely rare hardware failure wouldn't affect them.

With a comprehensive offsite backup plan, your devs will be able to overwrite any live site in seconds and get back to normality. Or restore backups on a separate staging server where they can experiment and make tweaks before pushing changes live.

Every Nimbus customer benefits from 14 offsite backup slots per website - updated every day at 2AM. Which means there's always a safe version of your site, sitting separately and securely on another server, ready for you to revert back to should you encounter any issues. **Plus, there's the option to upgrade to 28 slots, should you want even more peace of mind.**

What is a staging server?
In short, it's a clone of your website, on a separate server, where you can experiment with any new changes prior to pushing them live - meaning you can catch mistakes before they cause issues on your live website.

How to back up a WordPress website

Plugins like **UpdraftPlus** are commonly used by developers to take manual backups of their sites.

While a host would normally cover all of the website config located on their servers, a plugin might only cover the theme files, or other WordPress-specific features. On balance, how backups are undertaken is a matter of preference - although it is best practice to ensure they are done on a **regular schedule.**

You can choose to take an extra backup, whenever you like, with just the **click of a button on the Nimbus platform.**

We'd recommend doing so prior to making any major site changes, like installing a new plugin or pushing live a new feature.

Some hosting providers save their backups on site in their usual data centre, but that opens you up to potential loss of both site and backups. For this reason, it's important to check whether your **backups are being hosted offsite** when choosing a web hosting provider - and it's good practice to take **multiple backups in different locations**, just in case any were to fail.

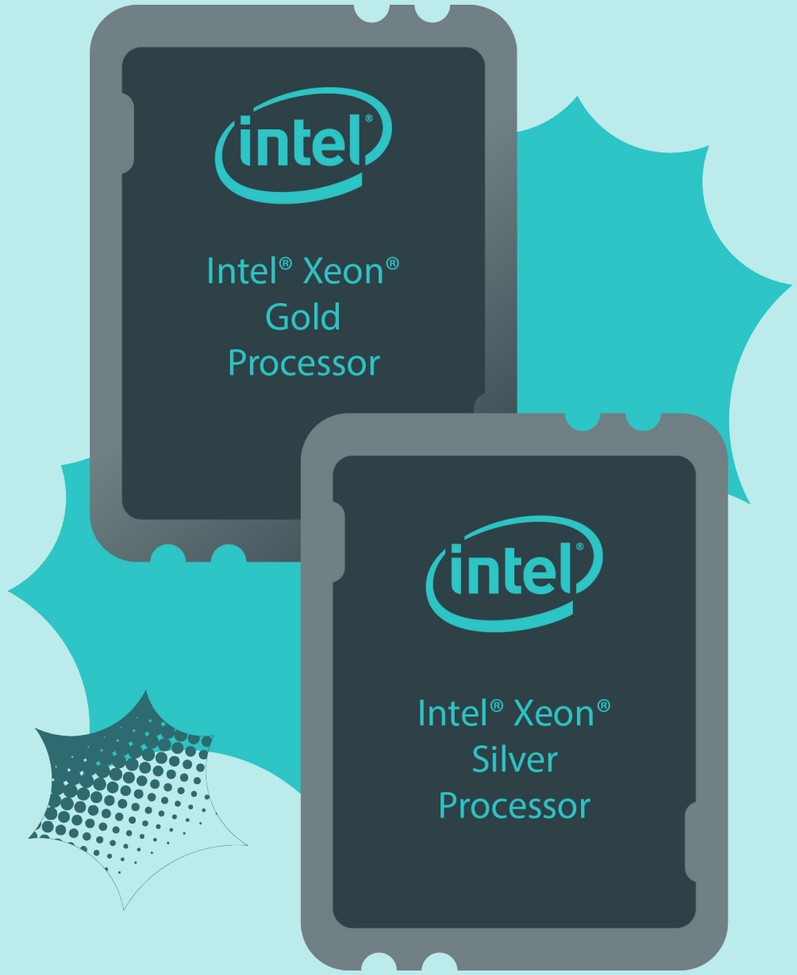
High-quality server hardware.

They say a worker is only as good as his tools, and that's certainly true of digital tools, too.

Outdated servers hosted within cheap data facilities can put your infrastructure under greater pressure, making it more vulnerable to security threats.

Conversely, the better the quality of your web hosting, the better the overall performance of your web portfolio. **Newer, better-managed hardware is more responsive, faster, and therefore ranks better with search engines** - ultimately picking up more traffic for your websites and improving your clients' reputation as market leaders.

The choice of a higher-quality web hosting provider also impacts security in a more direct manner, as a good host will champion their own features **designed to harden sites against attacks.**



At Nimbus, these include: running web services for each site as its own user, adding open_base_dir protection and firewall rules to protect non-web ports by default, and 2FA authentication for improved user security.

We're also proud of our specs:

- **High-performance HPE ProLiant Gen10 servers for security, agility and flexibility**
- **Intel® Xeon® processing power, with High-performance 2nd gen Intel® Xeon® Silver Scalable Processors**
- **Exceptional performance and consistently low latency through HPE SSDs - and enterprise-grade SSD storage**
- **All running in an ISO-accredited data centre, built from the ground-up to be eco-friendly**

Secure your sites, peace of mind, and happy clients.

The best approach to navigating security issues, attacks, hacks, and data loss within your site portfolio can be summed up by two words: prevention and automation.

By covering all bases as early as possible you can save yourself from the headache of troubleshooting your sites in the event of a security breach - or, at the very least, you can manage the level of possible damage which can be enacted during such a breach.

By automating your security measures to the greatest extent you're able to, you'll remove the danger of human error resulting in an issue.

Whether that's by neglecting to update a plugin or theme, or simply foregoing regular site backups, automation can protect your web portfolio by **closing vulnerabilities and creating contingencies** without requiring individual involvement.

After all, the less pressure placed on an individual to manage sites security, the better placed the overall security infrastructure to **withstand attacks and issues.**

That's why we've packed the intuitive Nimbus platform with dozens of security features to protect all your sites and servers.

Rest assured that our infrastructure has **security built in**, while **automatic features** protect your sites from common attacks. We've designed our platform specifically for agencies and developers, so it's easy to implement security features, take offsite backups, ensure PCI compliance, and so much more, in the flip of a toggle.

The best time to implement a thorough and effective security strategy is upon the **first set up of your sites** - the second best time is once you learn that you can do better.

By following the steps outlined in our **security checklist**, you can be confident that your sites are adequately protected against the majority of security threats - meaning more peace of mind for you, now and in the future.

CHECKLIST:

The Nimbus Site Security Checklist

Our best-practice model for site security ensures your security protocols are multi-faceted and more likely to effectively protect your clients from a range of security vulnerabilities and attacks.

- [ ] Set up Web Application Firewalls
- [ ] Manage your updates
- [ ] Install security plugins
- [ ] Create a multi-server environment
- [ ] Ecommerce site? Ensure you're PCI Compliant
- [ ] Undertake WordPress admin
- [ ] Take offsite backups
- [ ] Host on high-quality server hardware

If you have more questions about securing your multi-site portfolio, reach out to our friendly UK-based tech experts. We're here and ready to help.

Powerful, secure web hosting,

designed especially for agencies and freelancers.

Our green hosting doesn't just run on renewables, it's also reliable, secure and phenomenally fast. In fact, it's 400% more capable than the competition when you hit a traffic spike, with guaranteed 99.995% uptime.

One dashboard, everything you need.

When your clients need you, effortlessly manage every site, server, project, and domain; seamless workflow integration, security, and resilience built in, and your entire empire at your fingertips.

Green hosting you'll want to shout about.

Carbon neutral web hosting that's run on 100% renewables. From the data centre, right down to our solar-powered HQ, we're helping to save 45 million tonnes of CO2 every year (and the planet).

A team of experts, always on hand.

Our UK-based tech enthusiasts, loaded with knowledge, answer 97% of support tickets within an hour. That's game-changing support you can rely on.

Nimbus

Powerful web hosting, designed especially for agencies and freelancers.

Switch to a hosting platform that makes you look like a superhero.

We're ready to empower you. Contact our Sales team to learn more:

CONTACT US

0208 146 6797
sales@nimbushosting.co.uk
www.nimbushosting.co.uk

@NimbusHosting